ELSEVIER
Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 316 (2007) 109–132
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

The multiplicative Jordan decomposition in group rings, II

Alfred W. Hales [a,*], Inder Bir S. Passi [b,1], Lawrence E. Wilson [a]

[a] *Center for Communications Research, San Diego, CA 92121, USA*
[b] *Centre for Advanced Study in Mathematics, Panjab University, Chandigarh 160014, India*

Received 17 April 2006

Available online 14 August 2007

Abstract

We classify the finite 2-groups G whose integral group rings $\mathbb{Z}[G]$ have the multiplicative Jordan decomposition property. In addition to those cases already known, these include three further cases of order thirty-two and no others. We also give a theorem which severely restricts the structure of those finite groups G with $\mathbb{Z}[G]$ having this property which are not of order $2^a 3^b$ for some a, b.

Keywords: Integral group ring; Unit group; Semisimple element; Unipotent element; Jordan decomposition; Wedderburn decomposition; 2-Group

1. Introduction

Let $\mathbb{Q}[G]$ be the rational group algebra of a finite group G. Every element $\alpha \in \mathbb{Q}[G]$ has a unique additive Jordan decomposition $\alpha = \alpha_s + \alpha_n$ with $\alpha_s, \alpha_n \in \mathbb{Q}[G]$, α_s semisimple, α_n nilpotent and $\alpha_s\alpha_n = \alpha_n\alpha_s$. Furthermore, if α is a unit, then so is α_s, and α has a unique multiplicative Jordan decomposition $\alpha = \alpha_s\alpha_u$, with α_u unipotent and $\alpha_s\alpha_u = \alpha_u\alpha_s$; here $\alpha_u = 1 + \alpha_s^{-1}\alpha_n$. If $\alpha \in \mathbb{Z}[G]$, the integral group ring over G, then the semisimple component α_s does not always lie in $\mathbb{Z}[G]$. The integral group ring $\mathbb{Z}[G]$ is said to have the AJD property if $\alpha_s \in \mathbb{Z}[G]$ (and hence $\alpha_n \in \mathbb{Z}[G]$) for every $\alpha \in \mathbb{Z}[G]$, and to have the MJD property if α_s and $\alpha_u \in \mathbb{Z}[G]$ for every unit

* Corresponding author.
E-mail addresses: hales@ccrwest.org (A.W. Hales), ibspassi@yahoo.co.in (I.B.S. Passi), larry@ccrwest.org (L.E. Wilson).
[1] Senior Scientist, INSA.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2007.07.009

$\alpha \in \mathbb{Z}[G]$. If $\mathbb{Z}[G]$ has the AJD property, then in fact it will also have the MJD property. While the finite groups G for which $\mathbb{Z}[G]$ has the AJD property are completely characterized [HP] (also see Theorem 4 below), the complete characterization of finite groups G for which $\mathbb{Z}[G]$ has the MJD property is still open, and only some partial results are known [AHP2,Par,HP1]. In this paper,[2] which is a continuation of work in [AHP2], we give a complete characterization (in fact list) of finite 2-groups whose integral group rings have the MJD property. Since integral group rings of finite abelian groups have AJD, and therefore MJD, we need focus attention only on non-abelian groups. It may be recalled that the integral group rings of both the quaternion group of order 8 and the dihedral group of order 8 have the MJD property [AHP1]. Out of the nine non-abelian groups of order 16, the integral group rings of exactly five of them have the MJD property [AHP2,Par]. Our main result is that there are exactly three non-abelian groups of order 32 whose integral group rings have the MJD property but not the AJD property and, if G is a finite 2-group of order at least 64, then $\mathbb{Z}[G]$ has the MJD property (if and) only if G is a Hamiltonian group.

We also give a concluding result which places very strong restrictions on the structure of those finite groups G which are not of order 2^a3^b for some a, b and for which $\mathbb{Z}[G]$ has the MJD property. These groups G, if $\mathbb{Z}[G]$ does not already have the AJD property, must either be of the form $Q_8 \times C_p$ for an odd prime p, or be certain split extensions of C_p by C_{2^k} or C_{3^k} for some $k \geqslant 1$.

A crucial role in this investigation is played by our Theorem 8 which states that if G is a finite group such that $\mathbb{Z}[G]$ has the MJD property and $\alpha \in \mathbb{Z}[G]$ is a nilpotent element, then the components of α in the Wedderburn decomposition of $\mathbb{Q}[G]$ all lie in $\mathbb{Z}[G]$.

2. Jordan decomposition

Let k be a field and A a finite-dimensional algebra over k. An element $\alpha \in A$ is said to be:

(i) *unipotent* if the element $\alpha - 1$ is nilpotent, where 1 is the identity element of A;
(ii) *semisimple* if the minimal polynomial of α over k does not have repeated roots in the algebraic closure $\bar{k}$ of k.

For the reader's convenience, we recall the following well-known result (e.g., see [B, p. 80], or [SWe, p. 83]).

Theorem 1. *Let k be a perfect field and A a finite-dimensional algebra over k. Then every element $\alpha \in A$ possesses a unique* additive Jordan decomposition *over k*:

$$\alpha = \alpha_s + \alpha_n,$$

where α_s is semisimple, α_n is nilpotent and $\alpha_s\alpha_n = \alpha_n\alpha_s$.

Further, if $\alpha \in A$ is an invertible element, then α has a unique multiplicative Jordan decomposition *over k*:

[2] The main result (Theorem 28) of this paper was announced by the second author in a talk given at the International Conference on Number Theory and Discrete Geometry held in honour of Professor R.P. Bambah's 80th birthday at Panjab University, Chandigarh, India (30 November–3 December 2005).

$$\alpha = \alpha_s \alpha_u = \alpha_u \alpha_s$$

with α_s semisimple and α_u unipotent.

It may be mentioned here that Jordan decomposition may fail if the ground field is not perfect. Consider the following example from [BC]:

Let $F = \mathbb{F}_2(x)$ be the field of rational functions over the field $\mathbb{F}_2$ of two elements. Let V be a vector space over F of dimension 4 with basis $\{v_i\}_{i=1}^4$. Define the linear transformation $T : V \to V$ by setting

$$T(v_1) = v_2, \qquad T(v_3) = v_4, \qquad T(v_2) = xv_1, \qquad T(v_4) = v_1 + xv_3.$$

Then there is no decomposition of T into a sum of commuting semisimple and nilpotent linear mappings.

Definition 2. Let k be a perfect field. A subgroup G of $GL(n,k)$, the general linear group of degree n over k, is called *splittable* if, together with each matrix $g \in G$, we have $g_s, g_u \in G$.

This definition was proposed by A.I. Mal'cev in [Ma], where the study of complex and real solvable splittable Lie algebras (groups) was introduced for the first time.

It is clear that the intersection of splittable groups is splittable. Therefore, for every $G \subseteq GL(n,k)$, there exists a smallest splittable subgroup of $GL(n,k)$ containing G; let us denote this subgroup by G^*. If k is algebraically closed and x is an element of $GL(n,k)$, then $\{x_s,\ x_u\} \subseteq \overline{\langle x \rangle}$, the Zariski closure of $\langle x \rangle$ in $GL(n,k)$ (see [We, p. 92]).

Let G be a finite group of order n and view the unit group $\mathcal{U} := \mathcal{U}(\mathbb{Z}[G])$ as a subgroup of $GL(n,\mathbb{C})$, via the regular representation of G. Let $\bar{\mathcal{U}}$ denote the Zariski closure of $\mathcal{U}$ in $GL(n,\mathbb{C})$. Then we have:

$$\mathcal{U} \subseteq \mathcal{U}^* \subseteq \bar{\mathcal{U}}.$$

This suggests the following:

Problem. For a given finite group G, investigate properties of the groups, $\bar{\mathcal{U}}$, $\mathcal{U}^*$. In particular, when is $\mathcal{U} = \mathcal{U}^*$, i.e., when is $\mathcal{U}$ splittable (or equivalently, when does $\mathbb{Z}[G]$ have MJD)?

Of course the same problem can be raised for any subring of $\mathbb{C}$ as coefficients which is not a field. It may however be noted that when $\mathbb{Z}$ is replaced by the ring R of all algebraic integers, the analogous question is completely answered by the following:

Theorem 3. *For G a finite group and R the ring of all algebraic integers, the group ring $R[G]$ has MJD if and only if G is abelian.*

Proof. By Corollary 3.2 in [HLP], $R[G]$ has AJD if and only if G is abelian. Hence, if G is abelian, then MJD holds for $R[G]$; and if G is not abelian, then there is an element α in $R[G]$ whose semisimple part α_s does not lie in $R[G]$. In the latter case, to show that MJD fails in $R[G]$, it suffices to find an $x \in R$ so that the element $x1 + \alpha$ is invertible in $R[G]$, since its semisimple part will be $x1 + \alpha_s$.

Consider the regular representation ρ of $R[G]$ in $\mathbb{M}_n(R)$, where $n = |G|$, the cardinality of G, with respect to the basis of group elements. Then the element $x1 + \alpha$ will be invertible in $R[G]$ if and only if its image in $\mathbb{M}_n(R)$ has invertible determinant in R. But the equation $\det(\rho(x1 + \alpha)) = 1$ is a monic polynomial equation with coefficients in R, so it must have a solution x in R. This concludes the proof. □

3. Jordan decomposition in integral group rings

Let us recall some known results.

Theorem 4. *(See [HP].) AJD holds in $\mathbb{Z}[G]$ if and only if G is either*

(a) *abelian, or*
(b) *of the form $Q_8 \times E \times A$, where Q_8 is the quaternion group of order eight, E is an elementary abelian 2-group and A is an abelian group of odd order such that the multiplicative order of 2 modulo $|A|$ is odd, or*
(c) *a dihedral group D_{2p} of order $2p$, where p is an odd prime.*

It may be noted that groups G satisfying (a) or (b) above are precisely the groups for which $\mathbb{Q}[G]$ contains no nonzero nilpotents, i.e. $\mathbb{Q}[G]$ is a direct sum of division rings, so AJD holds in $\mathbb{Z}[G]$ for trivial reasons.

As mentioned earlier, if $\mathbb{Z}[G]$ has AJD then it must also have MJD. (This can be seen by using the uniqueness of AJD to show that $(\alpha_s)^{-1} = (\alpha^{-1})_s$ whenever α is invertible.) The converse, however, is not true. The following result provides examples of groups G where MJD but not AJD holds for $\mathbb{Z}[G]$.

Theorem 5. *(See [AHP2].)*

(a) *MJD holds in the integral group ring $\mathbb{Z}[D_{2n}]$ if and only if n is either 2, 4, or an odd prime, and*
(b) *MJD holds in the integral group $\mathbb{Z}[Q_{4p}]$ for all odd primes p, where Q_{4p} is the generalized quaternion group of order $4p$ presented by $\langle x, t \mid x^p = t^4 = 1, txt^{-1} = x^{-1}\rangle$.*

Just like the AJD property, the MJD property in the integral group ring $\mathbb{Z}[G]$ has a strong bearing on the Wedderburn structure of the rational group algebra $\mathbb{Q}[G]$.

Theorem 6. *(See [AHP2].) Let G be a finite group. Then, for MJD to hold in $\mathbb{Z}[G]$, it is necessary that the degrees of the Wedderburn components of $\mathbb{Q}[G]$ must all be less than or equal to 3.*

The above result is, in fact, best possible. Consider the following examples, the first from [Ar]. Let $G = \langle x, t \mid x^7 = t^3 = 1,\ txt^{-1} = x^2\rangle$. Let ω be a primitive cube root of unity. Then

$$\mathbb{Q}[G] \simeq \mathbb{Q} \oplus \mathbb{Q}(\omega) \oplus \mathbb{M}_3\big(\mathbb{Q}\sqrt{-7}\big),$$

and $\mathbb{Z}[G]$ has MJD.

Another example from [LP] is as follows.

Let G be either of the two non-abelian groups of order 27, $F = \mathbb{Q}[\omega]$, where ω is a primitive cube root of unity. Then:

(i) $\mathbb{Q}[G] \simeq \mathbb{Q} \oplus F^4 \oplus \mathbb{M}_3(F)$,
(ii) $\mathbb{Z}[G]$ has the MJD property.

As a result of Theorem 6, if neither 2 nor 3 divides the order of G, then $\mathbb{Z}[G]$ has MJD if and only if G is abelian. More generally, we have, by invoking [GH, Theorem 2.2].

Theorem 7. *If $\mathbb{Z}[G]$ has MJD, then there exists a normal abelian subgroup N in G such that $|G/N| = 2^a \cdot 3^b$ (a, b integers) and $|N|$ is not divisible by 2 or 3; in particular, G must be solvable.*

Theorem 29, in our concluding section, expands on and strengthens the above result substantially. To begin the present investigation of MJD, we note that this property is subgroup closed; i.e., if G is a finite group such that $\mathbb{Z}[G]$ has MJD and H is a subgroup of G, then $\mathbb{Z}[H]$ also has MJD. This follows from the uniqueness of Jordan decomposition. The following result about nilpotent elements in integral group rings with MJD plays a crucial role in our study.

Theorem 8. *Let G be a finite group such that the integral group ring $\mathbb{Z}[G]$ has MJD. Let*

$$\mathbb{Q}[G] = A_1 \oplus \cdots \oplus A_m$$

be the Wedderburn decomposition of the rational group algebra $\mathbb{Q}[G]$ with $A_i \simeq \mathbb{M}_{s_i}(D_i)$ ($i = 1, \ldots, m$), where the D_i's are division $\mathbb{Q}$-algebras. If $z = z_1 + z_2 + \cdots + z_m \in \mathbb{Z}[G]$ is nilpotent, with each $z_i \in A_i$, then $z_i \in \mathbb{Z}[G]$ for all i.

Proof. Suppose that $x \in \mathbb{M}_s(D)$ is a non-zero nilpotent element, where $s = 2$ or 3 and D is a division algebra containing $\mathbb{Q}$. Then we assert that there is a nilpotent element $y \in \mathbb{M}_s(D)$ such that $(I + x)(I + ny)$ is semisimple for all positive integers n, where I is the $s \times s$ identity matrix. Note that if any conjugate of x has the asserted property, then so has x. We can therefore assume, without loss of generality, that x is a Jordan matrix.

Suppose that $s = 2$ and $x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$. Take $y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. Let $M := (I + x)(I + ny) = \begin{pmatrix} n+1 & 1 \\ n & 1 \end{pmatrix}$, where n is a positive integer. For the matrix M to have equal eigenvalues, we must have $(\frac{n+2}{2})^2 = 1$, i.e., $n = 0$ or -4. Since this is not the case, M is a semisimple matrix.

Next suppose $s = 3$ and

$$\text{(i)} \quad x = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \text{or} \quad \text{(ii)} \quad x = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix}.$$

In case (i), take $y = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Then $(1 + x)(I + ny) = \begin{pmatrix} n+1 & 1 & 0 \\ n & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ which is easily seen to have distinct eigenvalues. In case (ii) take $y = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ so that

$$(I + x)(I + ny) = \begin{pmatrix} 1 & 1 & 0 \\ n & 1 & 1 \\ n & 0 & 1 \end{pmatrix}$$

which is again easily verified to be a semisimple matrix.

Let $1 = e_1 + \cdots + e_m$ where e_i's are central orthogonal primitive idempotents in $\mathbb{Q}[G]$ providing the given Wedderburn decomposition, and $z = z_1 + \cdots + z_m$, $z_i \in A_i$, a nilpotent element in $\mathbb{Z}[G]$. In order to show that $z_i \in \mathbb{Z}[G]$ for all $i = 1, \ldots, m$, it clearly suffices to consider the case when $i = 1$ and $s_1 = 2$ or 3 (see Theorem 6). In view of the above assertion, we can choose nilpotent $y_i \in A_i$ $(i > 1)$ so that $(e_i + z_i)(e_i + ny_i) \in A_i$ is semisimple for all positive integers n. Consider the element

$$y := 0 + y_2 + y_3 + \cdots + y_m \in \mathbb{Q}[G].$$

Choose an integer $N > 0$ such that $Ny \in \mathbb{Z}[G]$. Then the element

$$\alpha := (1 + z)(1 + Ny) \in \mathbb{Z}[G]$$

is a unit in $\mathbb{Z}[G]$ and clearly

$$\alpha_s = e_1 + (e_2 + z_2)(e_2 + Ny_2) + \cdots,$$
$$\alpha_n = z_1.$$

Since $\mathbb{Z}[G]$ has multiplicative Jordan decomposition, it follows that $z_1 \in \mathbb{Z}[G]$, and the theorem is proved. □

Note that the above theorem is equivalent to saying that if $\{e_1, \ldots, e_m\}$ is a complete set of orthogonal primitive central idempotents of $\mathbb{Q}[G]$, the ring $\mathbb{Z}[G]$ has MJD and $z \in \mathbb{Z}[G]$ is a nilpotent element, then $ze_i \in \mathbb{Z}[G]$ for all $i = 1, \ldots, m$.

The above theorem has a number of immediate consequences.

Corollary 9. *If $z \in \mathbb{Z}[G]$ is a nilpotent element, then $ze \in \mathbb{Z}[G]$ for all central idempotents $e \in \mathbb{Q}[G]$, provided $\mathbb{Z}[G]$ has MJD.*

Corollary 10. *Let G be a finite group, and suppose there exist a nontrivial normal subgroup K of G, and $y, z \in G$ such that $y^2 = 1$, $yzyK \neq zK$. Then G does not have MJD.*[3]

Proof. Consider the element

$$\alpha = (1 - y)z(1 + y)$$

of $\mathbb{Z}[G]$ and note that $\alpha \neq 0$, $\alpha^2 = 0$ and $\alpha\hat{K}/|K| \notin \mathbb{Z}[G]$, where $\hat{K}$ denotes the sum of all the elements of K. □

Corollary 11. *If G is a finite group such that $\mathbb{Z}[G]$ has MJD, then either*

(i) *every element of order two is central or*
(ii) *the center of G is cyclic* (*so there is a unique central element of order two*).

Proof. Suppose neither (i) nor (ii) holds. Then there exists an element y of order two such that $[y, G] \neq 1$. Since the center of G is not cyclic, there exist two central subgroups with trivial intersection. At least one of them does not contain $[y, G]$; call it K and choose $z \in G$ such that

[3] The referee has pointed out a strengthening of this corollary, namely, that it suffices to require only that y^2 not generate K, rather than $y^2 = 1$.

$[y, z] \notin K$. The conditions of Corollary 10 are then satisfied, giving the conclusion that $\mathbb{Z}[G]$ does not have MJD, which is a contradiction. □

Corollary 12. *If the group G has trivially intersecting subgroups N and H, where N is nontrivial and normal, and the group algebra $\mathbb{Q}[H]$ has nonzero nilpotent elements, then the integral group ring $\mathbb{Z}[G]$ does not possess MJD.*

Proof. Let $e = (\sum_{n \in N} n)/|N|$. Then e is a central idempotent in $\mathbb{Q}[G]$. If we take z to be a nonzero nilpotent element in $\mathbb{Z}[H] \backslash |N|\mathbb{Z}[H]$, then ze will not lie in $\mathbb{Z}[G]$ and the assertion follows from Corollary 9. □

This immediately yields the following result.

Corollary 13. *If the group algebra $\mathbb{Q}[G]$ has non-zero nilpotent elements, then the integral group ring $\mathbb{Z}[G \times C_p]$ does not possess MJD for any prime p.*

The above result raises the question of whether $\mathbb{Z}[Q_8 \times C_p]$, where p is an odd prime, can have MJD without having AJD. We show here that $\mathbb{Z}[Q_8 \times C_3]$ does in fact have MJD.

Let $Q_8 = \langle x, y \mid x^4 = 1, x^2 = y^2, x^{-1}yx = y^{-1}\rangle$, $C_3 = \langle t \mid t^3 = 1\rangle$. Suppose $u = \alpha + \beta t + \gamma t^2$, with $\alpha, \beta, \gamma \in \mathbb{Z}[Q_8]$, is an element of $\mathcal{U}(\mathbb{Z}[G])$ which is not semisimple. We can assume, without loss of generality, that the augmentation of u is 1. The units in $\mathbb{Z}[Q_8]$ as well as in $\mathbb{Z}[G_{ab}]$ are trivial (here G_{ab} denotes the commutator quotient G/G'). Therefore, when we substitute $t = 1$ (respectively go modulo the ideal generated by $(x^2 - 1)$) u reduces to a group element in Q_8 (respectively $(Q_8)_{ab} \times C_3$). Let ω be a primitive cube root of unity. Define $\rho : \mathbb{Z}[G] \to \mathbb{M}_2(\mathbb{Z}[\omega])$ by setting

$$x \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} \omega & \omega^2 \\ \omega^2 & -\omega \end{pmatrix}, \qquad t \mapsto \begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix}.$$

Observe that

$$\mathbb{Q}[G] \simeq \mathbb{M}_2\big(\mathbb{Q}(\omega)\big) \oplus \mathbb{Q}(\omega)^4 \oplus \mathbb{Q}^4 \oplus \mathbb{H},$$

where $\mathbb{H}$ is the rational quaternion algebra. Since u is a unit in $\mathbb{Z}[G]$, and is not semisimple, $\rho(u)$ must have equal eigenvalues ϵ, ϵ which are units in $\mathbb{Z}[\omega]$. Furthermore, by multiplying u by a central group element if necessary, we can guarantee that either its images in Q_8 and in $(Q_8)_{ab} \times C_3$ are both trivial or (up to symmetries of Q_8) $x, \bar{x}$. Hence the determinant ϵ^2 of $\rho(u)$ must be 1 modulo 2 in $\mathbb{Z}[\omega]$ so ϵ must be $+1$ or -1. There are thus four cases to consider, according to the sign of ϵ and whether the image of u in Q_8 is trivial. If ϵ is $+1$ and the image of u in Q_8 is trivial, then we conclude that u_s is 1 so it lies in the integral group ring. Next we consider the case when both eigenvalues ϵ of $\rho(u)$ equal -1 and the image of u is still trivial. Then we have

$$\alpha + \beta + \gamma = 1,$$
$$\alpha = 1 + \big(x^2 - 1\big)\alpha',$$
$$\beta = \big(x^2 - 1\big)\beta',$$

$$\gamma = (x^2 - 1)\gamma',$$

where $\alpha', \beta', \gamma' \in \mathbb{Z}[G]$. In this case, we have $\rho(u) = \begin{pmatrix} 1-2a & -2b \\ -2c & 1-2d \end{pmatrix}$ for some $a, b, c, d \in \mathbb{Z}[\omega]$. Therefore

$$\begin{aligned} -2 = \operatorname{Tr}(\rho(u)) &= \operatorname{Tr}(\rho(\alpha)) + \omega \operatorname{Tr}(\rho(\beta)) + \omega^2 \operatorname{Tr}(\rho(\gamma)) \\ &= 2 - 2\operatorname{Tr}(\alpha') - 2\omega \operatorname{Tr}(\beta') - 2\omega^2 \operatorname{Tr}(\gamma') \end{aligned}$$

where Tr denotes trace. Thus we have

$$\operatorname{Tr}(\rho(\alpha')) + \omega \operatorname{Tr}(\rho(\beta')) + \omega^2 \operatorname{Tr}(\rho(\gamma')) = 2.$$

Also, since $\alpha + \beta + \gamma = 1$, we have

$$\operatorname{Tr}(\rho(\alpha')) + \operatorname{Tr}(\rho(\beta')) + \operatorname{Tr}(\rho(\gamma')) = 0.$$

Since $\omega - 1$ does not divide 2 in $\mathbb{Z}[\omega]$, we have a contradiction, and so this case is not possible. The analysis in the other two cases is similar and is omitted.

The next instance of the preceding question, namely the group $Q_8 \times C_5$, is still open, but we do have the following lemma, which will be useful later on.

Lemma 14. *Let $Q_8 = \langle x, y, z, t \mid x^2 = y^2 = z^2 = t,\ t^2 = 1,\ xy = z,\ [x, y] = t\rangle$ be the quaternion group and let p be an odd prime so that the multiplicative order of 2 modulo p is even. Then taking $G = Q_8 \times C_{p^2}$, we have that $\mathbb{Z}[G]$ does not possess MJD.*

Proof. Since 2 has even multiplicative order modulo p we know that $\mathbb{Q}[Q_8 \times C_p]$ contains nonzero nilpotent elements, and we can hence find polynomials $q(X), r(X), s(X)$, not all zero, in $\mathbb{Z}[X]$ with $q(\alpha)^2 + r(\alpha)^2 + s(\alpha)^2 = 0$ where α is a primitive pth root of unity. Since the ideal $(1 - \alpha)$ is prime and principal in $\mathbb{Z}[\alpha]$ we can assume without loss of generality that not all of $q(\alpha), r(\alpha), s(\alpha)$ are divisible by $(1 - \alpha)$. Let c generate C_{p^2} and consider the following element w of $\mathbb{Q}[G]$ which actually lies in $\mathbb{Z}[G]$: $w = (1/p)(1 - t)[(1 - c)^{p^2-p-1}(1 - c^p)(q(c^p)x + r(c^p)y + s(c^p)z) - (1 - c)^{p-1}(1 + c^p + \cdots + c^{(p-1)p})(q(c)x + r(c)y + s(c)z)]$. If we multiply w by the central idempotent $e = (1/p)(1 + c^p + \cdots + c^{(p-1)p})$ the product is not in $\mathbb{Z}[G]$ so MJD must fail for $\mathbb{Z}[G]$. □

Two further lemmas will also be useful.

Lemma 15. *Let p be an odd prime and let G be the split extension of $C_p = \langle c\rangle$ by $Q_8 = \langle x, y, z, t\colon\ x^2 = y^2 = z^2 = t,\ t^2 = 1,\ xy = z,\ [x, y] = t\rangle$ with action $c^x = c^{-1}$ and $c^y = c$. Then MJD fails for $\mathbb{Z}[G]$.*

Proof. Consider the nilpotent element $\alpha = (1 - x)c(1 + x + x^2 + x^3)$ in $\mathbb{Z}[G]$ and the central idempotent $e = (1 + y + y^2 + y^3)/4$ in $\mathbb{Q}[G]$. Their product does not lie in $\mathbb{Z}[G]$ so MJD must fail by Corollary 9. □

Lemma 16. *Let p be an odd prime and k a positive integer, and let G be the split extension of $C_p \times C_p = \langle x\rangle \times \langle y\rangle$ by $C_{3^k} = \langle s\rangle$, where $x^s = y$ and $y^s = (xy)^{-1}$. Then MJD fails for $\mathbb{Z}[G]$.*

Proof. Consider the nilpotent element

$$\alpha = (1 - s)x\bigl(1 + s + s^2 + \cdots + s^{3^k - 1}\bigr)$$

in $\mathbb{Z}[G]$ and the central idempotent

$$e = \widehat{\langle x\rangle}/p + \widehat{\langle y\rangle}/p + \widehat{\langle xy\rangle}/p - 3\widehat{\langle x, y\rangle}/\bigl(p^2\bigr)$$

in $\mathbb{Q}[G]$. Their product does not lie in $\mathbb{Z}[G]$ so again Corollary 9 shows that MJD must fail. □

The investigation of the AJD property for integral group rings was greatly simplified due to the fact that this property passes on to quotients. If N is a normal subgroup of G and units from $\mathbb{Z}[G/N]$ can be lifted to units in $\mathbb{Z}[G]$, then, of course, the MJD property passes from G to G/N. However, in general, units do not lift for integral group rings which is the major obstruction. For, let $G \to H$ be an epimorphism of groups. Then the induced ring homomorphism $\mathbb{Z}[G] \to \mathbb{Z}[H]$ does not in general restrict to units to provide an epimorphism $\mathcal{U}(\mathbb{Z}[G]) \to \mathcal{U}(\mathbb{Z}[H])$. For example, consider the group

$$Q_{12} = \bigl\langle x, y \bigm| x^3 = y^4 = 1,\ x^y = x^{-1}\bigr\rangle,$$

and its quotient

$$D_6 = \bigl\langle \bar{x}, \bar{y} \bigm| \bar{x}^3 = \bar{y}^2 = 1,\ \bar{x}^{\bar{y}} = \bar{x}^{-1}\bigr\rangle,$$

Any nilpotent element in $u \in \mathbb{Z}[Q_{12}]$ is necessarily of the type:

$$\begin{aligned} u = {} & ay + bxy + (-a - b)x^2y \\ & + cy^{-1} + dxy^{-1} + (-c - d)x^2y^{-1} \\ & + e\bigl(x - x^{-1}\bigr) + f\bigl(xy^2 - x^{-1}y^2\bigr); \end{aligned}$$

for, in a nilpotent element the partial augmentations with respect to the conjugacy classes all vanish. Consider the homomorphism $\rho : \mathbb{Z}[Q_{12}] \to \mathbb{H}_{\mathbb{R}}$, the quaternion algebra over the reals, defined by $x \to \omega = \frac{-1+\sqrt{3}i}{2}$, $y \to j$. Since u is nilpotent, we have $\rho(u) = 0$, and consequently $a = c$, $b = d$, $e = f$. Therefore, the image $\bar{u} \in \mathbb{Z}[D_6]$ of u has the property that the coefficients of $\bar{x}$, $\bar{y}$, $\bar{x}\bar{y}$ are all even. Now observe that the element

$$v = 1 + \bigl(\bar{x} - \bar{x}^{-1}\bigr) + \bigl(\bar{y} - \bar{x}^2\bar{y}^{-1}\bigr)$$

is unipotent in $\mathbb{Z}[D_6]$. Suppose α is a lift of v in $\mathbb{Z}[Q_{12}]$. Since MJD holds in $\mathbb{Z}[Q_{12}]$, $\alpha = \alpha_s.\alpha_u$, and necessarily $\alpha_u \mapsto v$ and $\alpha_s \mapsto 1$. This would mean that $v - 1$ lifts to a nilpotent element which is not possible in view of the foregoing analysis.

Thus, in general, under an epimorphism $\mathbb{Z}[G] \to \mathbb{Z}[H]$ induced by an epimorphism $G \to H$ neither nilpotents nor units lift. This question does not seem to have been addressed in the literature.

For semisimple elements we have the following:

Theorem 17. *If $G \to H$ is an epimorphism of groups and $\alpha \in \mathbb{Z}[H]$ is a semisimple element, then α can be lifted to a semisimple element in $\mathbb{Z}[G]$.*

Proof. Suppose that the Wedderburn decomposition of $\mathbb{C}[G]$ is given by $R_1 \oplus R_2 \oplus \cdots \oplus R_m$ where each R_i is a full matrix ring over $\mathbb{C}$. Since $\mathbb{C}[H]$ is a homomorphic image of $\mathbb{C}[G]$ and each R_i is simple, we may assume that a compatible Wedderburn decomposition for $\mathbb{C}[H]$ is given by the direct sum of R_1 through R_k with $k < m$. Now let α be a semisimple element of $\mathbb{Z}[H]$. Then each component of α in an R_i, for i at most k, must be a semisimple matrix. Our task is to show that α can be lifted to an element β in $\mathbb{Z}[G]$ so that the component of β in each R_i for $i > k$ is also semisimple. We will in fact arrange for each such component to have distinct eigenvalues. Note that α can obviously be lifted to a semisimple element of $\mathbb{C}[G]$ since then the later components can be specified arbitrarily.

Fix now a set S of coset representatives for H in G and let T be the complement $G \setminus H$. The coefficients of elements of T in a lift β for α determine β completely, and the matrix entries of the image $\pi_i(\beta)$ in R_i, for $i > k$, are linear functions of these coefficients. The characteristic polynomial of this image matrix in R_i will have coefficients which are polynomials in the T-coefficients of β, and thus the discriminant of this characteristic polynomial will be a polynomial in these T-coefficients. Hence the condition that the image matrix have distinct eigenvalues amounts to the nonvanishing of a certain polynomial, for each $i > k$.

But these $m - k$ polynomials clearly have a common nonzero in $\mathbb{C}^T$ by our earlier comment. Since $\mathbb{Z}^T$ is Zariski dense in $\mathbb{C}^T$ they will have a common nonzero in $\mathbb{Z}^T$, thus providing the desired lift. $\square$

Question. Under what circumstances can semisimple units in $\mathbb{Z}[H]$ always be lifted to semisimple units in $\mathbb{Z}[G]$?

This question appears to be open even for abelian groups. Even though units may not always lift, it is still sometimes possible to relate MJD in $\mathbb{Z}[H]$ to MJD in $\mathbb{Z}[G]$ when H is a homomorphic image of G. This is illustrated in the following lemma, which will be useful later on.

Lemma 18. *Suppose that p is an odd prime and that k divides $p - 1$ where $k > 3$. Let H be the split extension of C_p by $C_k = \langle c \rangle$, where c has order k in its action by conjugation on C_p. Then if G is a finite group which has H as a homomorphic image, MJD must fail for $\mathbb{Z}[G]$.*

Proof. The group algebra $Q[H]$ has a degree k Wedderburn component. But this implies that $\mathbb{Q}[G]$ must also have a degree k component, since Wedderburn components are simple and $\mathbb{Q}[G]$ maps onto $\mathbb{Q}[H]$. Thus MJD fails for $\mathbb{Z}[G]$ by Theorem 6. $\square$

We now take up the investigation of the MJD property for the integral group rings of finite 2-groups. We identify the various groups of small order by their Hall–Senior number [HS].[4] The 2-groups of order $\leqslant 16$ have already been settled [AHP2,Par]. There are exactly seven non-abelian groups of order $\leqslant 16$ with integral groups having the MJD property; namely, D_8, Q_8, and

[4] We refer to [Index16,Index32,Index64] for presentations of these groups and their relevant containment relations. Note one mistake in these sites: the group 32.40 is a subgroup of group 64.187—this is given correctly in [Index64] but not in [Index32].

the groups with Hall–Senior numbers 16.7, 16.8, 16.10, 16.11, and 16.14. We thus begin with the characterization of groups of order 32 whose integral group rings have the MJD property.

Up to isomorphism, there are fifty-one groups of order 32, seven of them are abelian. A check on each of the forty-four non-abelian groups of order 32 yields the following:

Theorem 19. *Out of the forty-four non-abelian groups of order* 32, *the integral group rings of exactly the following four groups have the MJD property*:

- 32.9: $C_2 \times C_2 \times Q_8$.
- 32.15: $C_4 \times Q_8$.
- 32.17: $\langle a, b, c \mid a^8 = 1, a^2 = b^2 = c^2,\ a^b = a^5,\ c \text{ central}\rangle$.
- 32.43: *The central product* $D_8 * Q_8$ *of the dihedral and quaternion groups of order 8, with presentation* $\langle a, b, c, d \mid a^4 = b^2 = c^4 = d^4 = 1,\ a^2 = c^2 = d^2,\ ac = ca,\ ad = da,\ bc = cb,\ bd = db,\ a^b = a^{-1},\ c^d = c^{-1}\rangle$.

Proof.

Case 1. *Groups containing a subgroup whose integral group ring does not have the MJD property.*

Since the MJD property is subgroup closed, the integral group rings $\mathbb{Z}[G]$, with G of order 32 having a subgroup H of order 16 and $\mathbb{Z}[H]$ not possessing the MJD property, do not themselves have the MJD property. This rules out the following twenty-three groups:

- Groups containing 16.6: 32.8, 32.10, 32.23, 32.27, 32.33, 32.34, 32.36, 32.42, 32.44, 32.46, 32.47.
- Groups containing 16.9: 32.11, 32.14, 32.16, 32.37, 32.38, 32.39, 32.41.
- Groups containing 16.12: 32.49, 32.50.
- Groups containing 16.13: 32.24, 32.26, 32.45.

Case 2. *Groups having a direct summand whose integral group ring has non-zero nilpotent elements.*

In view of Corollary 13, the MJD property fails for the integral group rings of the following three groups:

32.12, 32.13, 32.25.

Case 3. *Groups whose integral group rings have nilpotent elements with non-integral Wedderburn components.*

We list the groups G whose integral group rings do not have the MJD property in view of Theorem 8. In each case we give a presentation of the group G, a non-zero nilpotent element $\alpha \in \mathbb{Z}[G]$, and a central idempotent $e \in \mathbb{Q}[G]$ such that $\alpha e \notin \mathbb{Z}[G]$. The verification every time is straightforward, and is therefore omitted.

32.18: $\langle a,\ b,\ c\colon a^2 = b^4 = c^4 = 1,\ ab = ba,\ ac = ca,\ bc = cba\rangle$.

$$\alpha = (1 + b + b^2 + b^3)c(1 - b), \quad e = (1 + c^2)/2.$$

32.19: $\langle a,\ b\colon a^8=b^4=1,\ ba=a^5b\rangle$.

$\alpha=a(1+b)(1+a^2b)(1-a^4)\in\mathbb{Z}[G],\quad e=(1-b^2)/2.$

32.20: $\langle a,\ b,\ c\colon a^8=1,\ b^2=a^4,\ b^a=bc,\ c$ central, $c^2=1\rangle$.

$\alpha=(a-ac)(1+b+b^2+b^3),\quad e=(1+a^2+a^4+a^6)/4.$

32.28: $\langle g_1,\dots,g_5\colon g_1^2=g_3, g_3^2=1,\ g_2^2=g_4^2=g_5,\ g_5^2=1,$

$[g_2,g_1]=g_4g_5,\ [g_4,g_1]=g_5,\ [g_4,g_2]=g_5,\ g_3$ central$\rangle$.

$\alpha=(g_2-1)g_1(1+g_2+g_2^2+g_2^3),\quad e=(1+g_3)/2.$

32.29: $\langle a,\ b \mid a^8=1=b^4,\ a^b=a^{-1}\rangle$.

$\alpha=(a-a^{-1})(1+b+b^2+b^3),\quad e=(1+a^4)/2.$

32.30: $\langle a,\ b\colon a^8=b^4=1,\ ab=ba^3\rangle$.

$\alpha=(a-a^3)(1+b+b^2+b^3),\quad e=(1+a^4)/2.$

32.31: $\langle a,\ b \mid a^4=1=b^8,\ [b,a]=a^2b^2,\ [b,a^2]=b^4\rangle$.

$\alpha=(1-a)b(1+a+a^2+a^3),\quad e=(1+b^4)/2.$

32.32: $\langle g_1,\dots,g_5\colon g_1^2=g_2^2=g_3,\ g_3^2=g_4^2=g_5,\ g_5^2=1,$

$[g_2,g_1]=g_4, [g_4,g_1]=g_5, [g_4,g_2]=g_5,\ g_3$ central$\rangle$.

$\alpha=(1-g_2)g_3g_4(1-g_5)+g_1(1+g_3)(1-g_4g_5)+g_1g_2(1+g_3)(1-g_4),$

and $e=(1-g_5)/2.$

32.35: $\langle g_1,\dots,g_5\colon g_1^2=g_2^2=g_4,\ g_4^2=1,\ g_3^2=g_5,\ g_5^2=1,\ [g_2,g_1]=g_4,$

$[g_3,g_2]=g_5,\ [g_1,g_3]=1\rangle$.

$\alpha=(1-g_2)g_3(1+g_2)(1+g_4),\quad e=(1+g_1+g_4+g_1g_4)/4.$

32.40: $\langle g_1,\dots,g_5\colon g_1^2=g_4g_5,\ g_2^2=g_5,\ g_3^2=g_4,\ g_4^2=g_5^2=1,\ [g_3,g_1]=g_4,$

$[g_3,g_2]=g_5,\ [g_1,g_2]=1\rangle$.

$\alpha=(g_3+g_1g_3+g_2g_3-g_1g_2g_3g_4)(1-g_5),\quad e=(1+g_4)/2.$

32.48: $\langle a,b,c\colon a^2=1=b^8=[c,a],\ c^2=b^4,\ [b,a]=b^4,\ [b,c]=ab^4\rangle$.

$\alpha=(b-ab)(1+c)(1+b^4),\quad e=(1-a)(1+b^4)(1+b^2)/8.$

32.51: $\langle a,\ b \mid a^{16}=1,\ a^8=b^2,\ a^b=a^{-1}\rangle$.

$\alpha=(a-a^{-1})(1+b+b^2+b^3),\quad e=(1+a^4+a^8+a^{12})/4.$

Case 4. *The groups* 32.21 *and* 32.22.

The integral group rings of these two groups do not have the MJD property. The group 32.21 is given by the presentation $\langle x,\ y\colon\ x^8 = y^4 = 1,\ [x, y] = y^2\rangle$. We note that the element

$$u = \bigl(2 + y + xy + x^2y\bigr) + \bigl(-1 + x^3y\bigr)x^4 + \bigl(-y - x^2y - x^3y\bigr)y^2 + (-xy)x^4y^2$$

is a unit in its integral group ring with

$$\begin{aligned} u^{-1} = {} & \bigl(2 - y - xy - x^2y\bigr) + \bigl(-1 - x^3y\bigr)x^4 \\ & + \bigl(y + x^2y + x^3y\bigr)y^2 + (xy)x^4y^2, \end{aligned}$$

and nilpotent component

$$u_n = (1/2)(y + xy)\bigl(1 + x^2\bigr)\bigl(1 + x^4\bigr)\bigl(1 - y^2\bigr) \notin \mathbb{Z}[G].$$

The group 32.22 is given by the presentation

$$\bigl\langle a,\ b \bigm| a^{16} = b^2 = 1,\ b = aba^7\bigr\rangle.$$

This group is a special case of a more general class of 2-groups dealt with later in Proposition 22. MJD fails for the integral group ring of this group. For, let $G = \langle a,\ b \mid a^{16} = b^2 = 1,\ b = aba^7\rangle$, and consider the element

$$u = 1 + 2(1 + b)\bigl(1 - a^4\bigr)\bigl(1 + a^8\bigr) + \bigl(2 + a^8\bigr)(1 + b)\bigl(a + a^7\bigr)\bigl(1 - a^4\bigr) \in \mathbb{Z}[G].$$

One can check that u is a unit in $\mathbb{Z}[G]$:

$$u^{-1} = 1 + 2(1 + b)\bigl(1 - a^4\bigr)\bigl(1 + a^8\bigr) - \bigl(2 + a^8\bigr)(1 + b)\bigl(a + a^7\bigr)\bigl(1 - a^4\bigr)$$

and its nilpotent part $u_n = \frac{1}{2}(1 + b)(a + a^7)(1 - a^4)(1 - a^8) \notin \mathbb{Z}[G]$.

Finally we are left with four groups of order 32; namely, 32.9, 32.15, 32.17, and 32.43. We assert that the integral group rings of all four of them have the MJD property.

Case 5. *Groups whose integral group rings have the MJD property.*

The group 32.9 is the Hamiltonian group of order 32; its rational group algebra does not have nilpotent elements and therefore the MJD property trivially holds in its integral group ring.

$$32.15\colon\quad G = \bigl\langle x, y, t\colon\ x^4 = t^4 = 1,\ x^2 = y^2,\ x^y = x^{-1},\ [x, t] = [y, t] = 1\bigr\rangle.$$

This group is the direct product $Q_8 \times C_4$. Its rational group algebra has the following Wedderburn decomposition:

$$\mathbb{Q}[G] \simeq \mathbb{M}_2\bigl(\mathbb{Q}(i)\bigr) \oplus \mathbb{Q}(i)^4 \oplus \mathbb{Q}^8 \oplus \mathbb{H} \oplus \mathbb{H}.$$

Let $u = \alpha + \beta t + \gamma t^2 + \delta t^3$, with $\alpha, \beta, \gamma, \delta$ in $\mathbb{Z}[Q_8]$ be a unit in $\mathbb{Z}[G]$. Clearly the image of u in each $\mathbb{Q}$ component and in each $\mathbb{Q}(i)$ component will be ± 1 or $\pm i$. Since the subquotient $\mathbb{Z}[Q_8 \times C_2]$ has trivial units, the image of u in each $\mathbb{H}$ component will also have multiplicative order (dividing) 4. To establish MJD for the unit u, we need consider only the case when u is not semisimple. Let $\rho : \mathbb{Q}[G] \to \mathbb{M}_2(\mathbb{Q}(i))$ be the representation given by

$$x \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad t \mapsto \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}.$$

Then $\rho(u)$ will have equal eigenvalues which must lie in $\mathbb{Z}[i]$ and be units there, so these eigenvalues must be ± 1 or $\pm i$. Multiplying u by a central element, if necessary, and using the fact that the subquotient $\mathbb{Z}[C_2^2 \times C_4]$ of $\mathbb{Q}[G]$ has trivial units, we can assume that

$$\begin{aligned} \alpha &= g + \left(x^2 - 1\right)\alpha', \\ \beta &= \left(x^2 - 1\right)\beta', \\ \gamma &= \left(x^2 - 1\right)\gamma', \\ \delta &= \left(x^2 - 1\right)\delta' \end{aligned}$$

for some $g \in G$ and α', β', γ', δ' in $\mathbb{Z}[Q_8]$. Now observe that $(u^4 - 1)^2 = 0$ and $u^4 - 1$ is a multiple of 4 in $\mathbb{Z}[G]$. It is easy to see that the semisimple part u_s of u lies in $\mathbb{Z}[G]$, since we may calculate that $u_s = u(u^4 - 1)/4$.

$$32.17: \quad G = \left\langle x,\ y,\ z\colon\ x^8 = 1,\ x^2 = y^2 = z^2,\ x^y = x^5,\ z \text{ central}\right\rangle.$$

Note that the commutator subgroup $G' = \langle x^4 \rangle$ is of order 2, and the center of G is $\langle z \rangle$ having order 8. The Wedderburn decompositions of the complex group algebra $\mathbb{C}[G]$ and the rational group algebra $\mathbb{Q}[G]$ are given as follows:

$$\begin{aligned} \mathbb{C}[G] &\simeq \mathbb{C}^{16} \oplus \mathbb{M}_2(\mathbb{C})^4; \\ \mathbb{Q}[G] &\simeq \mathbb{Q}^8 \oplus \mathbb{Q}(i)^4 \oplus \mathbb{M}_2\left(\mathbb{Q}(\epsilon)\right), \end{aligned}$$

where ϵ is a primitive 8th root of unity. Consider the representation $\varphi : \mathbb{Q}[G] \to \mathbb{M}_2(\mathbb{Q}(\epsilon))$ defined by

$$x \mapsto \begin{pmatrix} 0 & 1 \\ i & 0 \end{pmatrix}, \qquad y \mapsto \begin{pmatrix} 0 & i \\ 1 & 0 \end{pmatrix}, \qquad z \mapsto \begin{pmatrix} \epsilon & 0 \\ 0 & \epsilon \end{pmatrix}.$$

For every element $\alpha \in \mathbb{Z}[G]$, $\mathrm{Tr}(\varphi(\alpha)) \equiv 0 \pmod 2$ in $\mathbb{Z}[\epsilon]$, where Tr denotes trace.

Suppose $\alpha \in \mathbb{Z}[G]$ is a unit of augmentation 1. Going modulo G', we see that α must be a trivial unit. Therefore, $\alpha = g + (1 - x^4)h$, for some $g \in G$, $h \in \mathbb{Z}[G]$. Consequently,

$$\mathrm{Tr}\left(\varphi(\alpha)\right) \equiv 0 \text{ or } 2u \mod 4,$$

where u is an 8th root of unity. Suppose the unit α is *not* semisimple. Then $\varphi(\alpha)$ necessarily has a repeated eigenvalue, say, v. Therefore,

$$2v \equiv 0 \text{ or } 2u \mod 4;$$

i.e.,

$$v \equiv 0 \text{ or } u \mod 2.$$

Since α is a unit, v is a unit in $\mathbb{Z}[\epsilon]$. Hence

$$v = \epsilon^k \cdot \left(1 + \epsilon + \epsilon^2\right)^l \quad (k, l \in \mathbb{Z}).$$

It then follows that l must be even. Hence v lies in a subgroup V of index 2 in the unit group of $\mathbb{Z}[\epsilon]$. The subgroup V is, in fact, the image of the homomorphism

$$\mathcal{U}\big(\mathbb{Z}[C_8]\big) \to \mathcal{U}\big(\mathbb{Z}[\epsilon]\big)$$

defined by $\lambda \mapsto \epsilon$, where λ is the generator of the cyclic group C_8. It follows that there exists an invertible element $w \in \mathbb{Z}[\langle z\rangle]$ whose image under φ is $\left(\begin{smallmatrix} v & 0 \\ 0 & v \end{smallmatrix}\right)$. Replacing α by αw^{-1} we can therefore assume that $v = 1$. We now note, by comparing the images in each component of $\mathbb{Q}[G]$, that the nilpotent component α_n of α is $(\alpha^4 - 1)/4$.

We claim that $\alpha_n \in \mathbb{Z}[G]$. For, observe that since $\alpha = g + (1 - x^4)h$ with $g \in G, h \in \mathbb{Z}[G]$, we have $\alpha^2 = g^2 + 2(1 - x^4)h'$ with $h' \in \mathbb{Z}[G]$. Therefore, $\alpha^4 = 1 + 4(1 - x^4)h''$ for some $h'' \in \mathbb{Z}[G]$. We have thus shown that α has MJD.

32.43: $G = D_8 * Q_8$, the direct product of D_8 and Q_8 with their centers amalgamated. This group has presentation $\langle a,\ b,\ c,\ d\colon\ a^4 = b^2 = c^4 = d^4 = 1,\ a^2 = c^2 = d^2,\ ac = ca,\ ad = da,\ bc = cb,\ bd = db,\ a^b = a^{-1},\ c^d = c^{-1}\rangle$.

We first note that

$$\mathbb{Q}[G] \simeq \mathbb{Q}^{16} \oplus \mathbb{M}_2(\mathbb{H}), \qquad \mathbb{C}[G] \simeq \mathbb{C}^{16} \oplus \mathbb{M}_4(\mathbb{C}).$$

On factoring by the normal subgroup $\langle a^2\rangle$, we get an elementary abelian group of order 16. Therefore in the Wedderburn decomposition of $\mathbb{Q}[G]$, there are 16 copies of $\mathbb{Q}$. The 2×2 matrix component corresponds to the representation

$$\rho : G \to \mathbb{M}_2(\mathbb{H})$$

given by

$$a \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad b \mapsto \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad c \mapsto \begin{pmatrix} i & 0 \\ 0 & i \end{pmatrix}, \qquad d \mapsto \begin{pmatrix} j & 0 \\ 0 & j \end{pmatrix}.$$

The above representation coupled with the embedding $\mathbb{H} \to \mathbb{M}_2(\mathbb{C})$ defined by

$$i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

provides a four-dimensional complex representation

$$\theta : G \to \mathbb{M}_4(\mathbb{C}).$$

Let χ be the character of the representation θ. Extend χ to $\mathbb{C}[G]$ by linearity. From the character table for G, we see that

$$\chi(g) \equiv 0 \mod 4 \quad \text{for all } g \in G.$$

Therefore $\chi(\alpha) \equiv 0 \bmod 4$ for all $\alpha \in \mathbb{Z}[G]$. Clearly $\theta(\mathbb{Z}[G]) \subseteq \mathbb{M}_4(\mathbb{Z}[i])$.

Let $\alpha \in \mathbb{Z}[G]$ be a unit. Then $\det(\theta(\alpha))$ is a unit in $\mathbb{Z}[i]$. Consider the element $\rho(\alpha) = \left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right)$, say, as an element in $M_2(\mathbb{H}_\mathbb{R})$, the real quaternions. We claim that, up to similarity over $\mathbb{H}_\mathbb{R}$, $\rho(\alpha)$ is an upper-triangular matrix, i.e., $u = 0$. This follows from a straightforward calculation, using the result that $\mathbb{H}_\mathbb{R}$ is 'algebraically closed' (see [L, Theorem 16.14]); this result is needed to show that the quadratic $X^2 - X(s + v^u) + (sv^u - tu)$ has a solution.

Taking a 'further conjugate,' if necessary, we can assume that $\rho(\alpha)$, up to a conjugate, is equal to $\left(\begin{smallmatrix} s & t \\ 0 & v \end{smallmatrix}\right)$ with $s,\ v \in \mathbb{C}$. Then the image of this matrix in $M_4(\mathbb{C})$ is

$$\begin{pmatrix} s & 0 & * & * \\ 0 & \bar{s} & * & * \\ 0 & 0 & v & 0 \\ 0 & 0 & 0 & \bar{v} \end{pmatrix}.$$

Its characteristic polynomial is $(X^2 - (s + \bar{s})X + s\bar{s})(X^2 - (v + \bar{v})X + v\bar{v})$, so $s + \bar{s} + v + \bar{v}$ is in $\mathbb{Z}$ (in fact in $4\mathbb{Z}$) and $s\bar{s}v\bar{v} = \pm 1$.

Suppose now that our unit $\alpha \in \mathbb{Z}[G]$ is not semisimple.

Then the characteristic polynomial of the matrix $A := \theta(\alpha)$ must have repeated roots, so either at least one of s, v is real or $s = v$. But if s is real and v is not, then $(X - s)(X^2 - (v + \bar{v})X + v\bar{v})$ is easily seen to annihilate the matrix. Similar is the case if v is real and s not. If both are real and unequal then the polynomial $(X - s)(X - v)$ annihilates A. Hence we must have $s = v$.

If $s = v$ is real, then s must be ± 1 since the determinant of A is ± 1. Thus the semisimple part of α is similar to (and hence equal to) the central element which is $\pm I$ in the matrix component $M_2(\mathbb{H})$ and ± 1 elsewhere. We can therefore, without loss of generality, assume that this is $+I$ in the matrix component by multiplying α by the central element a^2 in G, if necessary. Now it is easy to calculate, component by component, that the nilpotent part α_n of α must be given by the polynomial $(X^2 - 1)/2$, i.e. $\alpha_n = (\alpha^2 - 1)/2$. We must show this lies in $\mathbb{Z}[G]$.

Now G mod $\langle a^2 \rangle$ is of exponent 2, so has trivial units. This means we may assume that α (or $-\alpha$) is of the form $g + (1 - a^2)\beta$ with g in G, β in $\mathbb{Z}[G]$. If g has order 2, then squaring this and subtracting 1 gives an element (of $\mathbb{Z}[G]$) which is clearly divisible by 2, so α_n lies in $\mathbb{Z}[G]$. The only problem is if g has order 4. But in that case, checking traces, we see that each element g of order 4 in G has image in $\mathbb{M}_4(\mathbb{C})$ with trace 0 (see the character table), and any element of the form $(1 - a^2)\beta$ has trace divisible by 8. So in this case the trace of (the image of) α under θ has trace divisible by 8. But, on the other hand, the trace of the image of α must be 4. This is a contradiction.

Finally, we must deal with the case $s = v$ not real, say $s = v = l + mi$. We have that $s\bar{s} = 1$, and $s + \bar{s} = 2l$. But $s + \bar{s} + v + \bar{v} = 4l$ lies in $4\mathbb{Z}$, so l is in $\mathbb{Z}$. Hence s satisfies the polynomial $X^2 - 2lX + 1$ with integral coefficients. This means $s = l \pm \sqrt{l^2 - 1}$. For s to not be real we have $l = 0$ and s must be i (or $-i$).

We now know that α has image ± 1 in all one-dimensional components and that its image in the matrix component $M_2(\mathbb{H})$ has semisimple part similar to iI. A straightforward calculation shows that the nilpotent part of α must then be given by the polynomial $X(X^4 - 1)/4$, i.e. we have

$\alpha_n = \alpha(\alpha^4 - 1)/4$. As above, we use the triviality of units for $G/\langle a^2\rangle$ to write $\alpha = g + (1 - a^2)\beta$ with g in G, β in $\mathbb{Z}[G]$. Squaring this twice and subtracting 1 clearly gives an element divisible by 4 in $\mathbb{Z}[G]$, so α_n lies in $\mathbb{Z}[G]$ and it follows that $\mathbb{Z}[G]$ has the MJD property.

This completes the analysis of all groups of order 32 and our theorem is thus proved. □

The above analysis for groups of order 32 shows that MJD is a very restrictive property. This is further corroborated by a similar but more tedious analysis for groups of order 64 which leads to the following.

Theorem 20. *Let G be a group of order* 64. *Then $\mathbb{Z}[G]$ has the MJD property if and only G is a Hamiltonian group.*

Proof. Suppose that G has order 64 and $\mathbb{Z}[G]$ has the MJD property. Then the latter is true for all subgroups of G, so either G has all its proper subgroups abelian or G has one of the four groups 32.9, 32.15, 32.17, or 32.43 as a subgroup. The first alternative will be covered by the two propositions and three lemmas immediately below. Consider the second alternative. There are 63 groups of order 64 which contain one of these four groups as a subgroup, one of which is Hamiltonian. We dispose of the other 62 cases by listing sixteen groups of order 32 where MJD fails for their integral group ring so that every one of the 62 cases contains one of these:

- Groups containing 32.8: 64.44.
- Groups containing 32.10: 64.14, 64.21, 64.27, 64.104, 64.105, 64.109, 64.111, 64.158, 64.159.
- Groups containing 32.11: 64.72.
- Groups containing 32.12: 64.19.
- Groups containing 32.13: 64.125.
- Groups containing 32.16: 64.79, 64.80, 64.107, 64.108, 64.115, 64.167, 64.168, 64.178, 64.179.
- Groups containing 32.18: 64.87, 64.145, 64.147.
- Groups containing 32.19: 64.101, 64.118, 64.119, 64.122.
- Groups containing 32.21: 64.35, 64.63, 64.206, 64.220, 64.222.
- Groups containing 32.22: 64.36, 64.66.
- Groups containing 32.25: 64.45.
- Groups containing 32.26: 64.241, 64.242, 64.243.
- Groups containing 32.28: 64.48, 64.56, 64.57, 64.203, 64.204.
- Groups containing 32.32: 64.58, 64.256, 64.257, 64.258.
- Groups containing 32.35: 64.70, 64.155, 64.156, 64.161, 64.162, 64.210, 64.211, 64.212, 64.264.
- Groups containing 32.39: 64.74, 64.165, 64.172, 64.263. □

To conclude our investigation of the MJD property for the integral group rings of finite 2-groups, we need to consider the non-abelian groups all whose maximal subgroups are abelian. A characterization of such groups is provided by the following result.

Proposition 21. *(See [Rédei].) Let G be a non-abelian p-group, all of whose maximal subgroups are abelian. Then G is one of the following groups*:

- *$G = Q_8$, the quaternion group of order* 8.
- *$G = \langle x, y\rangle$ with defining relations*

$$x^{p^a} = y^{p^b} = 1, \quad x^y = x^{1+p^{a-1}} \quad (a \geqslant 2,\ b \geqslant 1); \qquad |G| = p^{a+b}.$$

- *$G = \langle x, y\rangle$ with the defining relations*

$$x^{p^a} = y^{p^b} = z^p = 1, \quad [x, y] = z; \qquad |G| = p^{a+b+1}.$$

Let

$$G\left(2^i, 2^j\right) = \left\langle x,\ y \;\middle|\; x^{2^i} = y^{2^j} = 1,\ [x, y] = x^{2^{i-1}}\right\rangle.$$

Then, as already noted, MJD holds for $\mathbb{Z}[G(4,2)]$ and $\mathbb{Z}[G(8,2)]$; we next prove that it fails for $\mathbb{Z}[G(2^i,2)]$ if $i > 3$.

Proposition 22. *Let G be a group of order 2^n, $n \geqslant 5$, with presentation*

$$\left\langle x, y \;\middle|\; x^{2^{n-1}} = 1 = y^2,\ x^y = x^{2^{n-2}+1}\right\rangle. \tag{1}$$

Then $\mathbb{Z}[G]$ does not have MJD.

Proof. For $n \geqslant 5$, define the integers $a := a(n)$ and $b := b(n)$ recursively by setting

$$a(5) = 2, \qquad a(n+1) = 2^{n-3} \cdot 9 \cdot b(n)^2 \quad \text{for } n \geqslant 5, \quad \text{and}$$
$$b(5) = 1, \qquad b(6) = 17, \qquad b(n+2) = b(n+1) \cdot \left(2^{2n-4} \cdot 9 \cdot b(n)^2 + 1\right) \quad \text{for } n \geqslant 5.$$

Consider the elements

$$v = (1+y)\left(1 - x^4\right) \prod_{i=3}^{n-2} \left(1 + x^{2^i}\right), \quad \text{and}$$
$$w = (1+y)\left(x + x^{2^{n-2}-1}\right)\left(1 - x^4\right) \prod_{i=3}^{n-3} \left(1 + x^{2^i}\right)\left(2 + x^{2^{n-2}}\right)$$

of $\mathbb{Z}[G]$, where the group G is given by the presentation (1). We claim that the element

$$u = 1 + av + bw$$

is a unit in $\mathbb{Z}[G]$, with $u^{-1} = 1 + av - bw$, and having semisimple part $u_s = u + (1/2)b(3\sigma - 2w)$ *not* in $\mathbb{Z}[G]$, where

$$\sigma = (1+y)\left(x + x^{2^{n-2}-1}\right)\left(1 - x^4\right) \prod_{i=3}^{n-2} \left(1 + x^{2^i}\right).$$

Simple computations in $\mathbb{Z}[G]$ show that we have:

$$\begin{cases} v^2 = 2^{n-2}v, \quad vw = 3 \cdot 2^{n-3}\sigma = wv, \quad v\sigma = 2^{n-2}\sigma = \sigma v, \\ w^2 = 9 \cdot 2^{n-3}v, \quad w\sigma = 3 \cdot 2^{n-2}v = \sigma w, \quad \text{and} \quad \sigma^2 = 2^{n-1}v. \end{cases} \tag{2}$$

Proceeding by induction on $n \geqslant 5$, taking the cases $n = 5$ and $n = 6$ as base cases, we note that

$$2^{n-3}a(n)^2 + a(n) = 9 \cdot 2^{n-4}b(n)^2 \quad \text{for all } n \geqslant 5. \tag{3}$$

With the help of Eqs. (2) and (3) one checks that

$$u(1 + av - bw) = 1,$$

and so u is a unit. Furthermore, these equations imply that the minimal polynomial of u is $(X-1)^2(X^2 - (2 + 2^{n-1}a)X + 1)$. We now compute the semisimple part of u by the method used in proving Proposition 2.1 in [AHP2] and obtain that

$$u_s = u + (1/2)b(3\sigma - 2w).$$

One quickly confirms that b is odd and that the coefficient of x in $3\sigma - 2w$ is 1. We thus conclude that the semisimple part of u has non-integer coefficients, finishing the proof of the proposition. $\square$

Lemma 23. *MJD fails for* $\mathbb{Z}[G(2^i, 2^j)]$ *whenever* 2^i *is at least* 8 *and* 2^j *is at least* 4.

Proof. Consider the elements A and B of $\mathbb{Z}[G]$ given by

$$A = \left(1 + x^{2^{i-2}}\right)x\left(x^{2^{i-1}} + y\right)\left(1 - x^{2^{i-1}}\right)\left(1 + y^2\right)\left(1 + y^4\right)\cdots\left(1 + y^{2^{j-1}}\right),$$
$$B = \left(1 + x^{2^{i-2}}\right)x\left(x^{2^{i-2}} + y\right)\left(1 - x^{2^{i-1}}\right)\left(1 - y^2\right)\left(1 + y^4\right)\cdots\left(1 + y^{2^{j-1}}\right).$$

It is straightforward to check that

$$A^2 = B^2 = AB = BA = 0,$$

and that $A + B$ lies in $2\mathbb{Z}[G]$. Now let $n = (A + B)/2$ which lies in $\mathbb{Z}[G]$. We have $n^2 = 0$, so n is nilpotent, but $ne \notin \mathbb{Z}[G]$, where $e = (1 + y^2)(1 + y^4)\cdots(1 + y^{2^{j-1}})/2^{j-1}$, a central idempotent. So MJD fails. $\square$

As noted earlier, MJD holds for the integral group ring of $G(4, 4)$ which is Hall–Senior group 16.10, and fails for the integral group ring of $G(4, 8)$ which is Hall–Senior group 32.21. We also have

Lemma 24. *MJD fails for* $\mathbb{Z}[G(4, 2^j)]$ *when* $2^j \geqslant 16$.

Proof. Consider the elements A, B of $\mathbb{Z}[G]$ given by

$$A = \left(1 + y^{2^{j-3}}\right)\left(1 + y^{2^{j-2}}\right)\left(x + y^{2^{j-2}}\right)y\left(1 - x^2\right)\left(1 - y^{2^{j-1}}\right),$$
$$B = \left(1 + y^{2^{j-3}}\right)\left(x + y^{2^{j-3}}\right)y\left(1 - x^2\right)\left(1 - y^{2^{j-2}}\right)\left(1 + y^{2^{j-1}}\right).$$

We proceed as in the proof of the preceding result, using the central idempotent $e = (1 - y^{2^{j-1}})/2$ or $(1 - y^{2^{j-2}})(1 + y^{2^{j-1}})/4$. $\square$

Lemma 25. *Let $G = \langle x, y, z \mid x^{2^i} = y^{2^j} = z^2 = 1,\ [x, y] = z$ central$\rangle$. If either 2^i or 2^j is at least* 4*, then $\mathbb{Z}[G]$ does not have MJD.*

Proof. We assume, without loss of generality, that $2^i \geqslant 4$. Consider the element

$$n = (x - xz)(1 + y)\left(1 + y^2\right) \cdots \left(1 + y^{2^{j-1}}\right).$$

It is straightforward to check that n is nilpotent. However, on multiplying n by the central idempotent $e = (1 + x^{2^{i-1}})/2$, we note that $ne \notin \mathbb{Z}[G]$. Hence MJD fails for the given group. $\square$

Note that taking $i = j = 1$ in the above lemma gives the dihedral group D_8, where MJD does hold for the integral group ring. Also note that this lemma completes the proof of Theorem 20.

Lemma 26. *If G is a* 2*-group having an abelian normal subgroup H such that $[G : H] = 2$ and* $\operatorname{rank}(H) \geqslant 3$*, then MJD holds in $\mathbb{Z}[G]$ only when AJD holds, i.e., when G is a Hamiltonian* 2*-group.*

Proof. Choose t in the complement $G \setminus H$ and consider the action of t by conjugation on the socle V of H, i.e. the elements of order two—a vector space over the two-element field. Since the action has order two, all Jordan blocks of V under this action will be of dimension one or two. Suppose first that there is a block of dimension two, generated by say x. Since H has rank three or more, there will also be a nontrivial element z in V, not in the block generated by x, which commutes with t. But then $(1 - x)t(1 + x)$ will be a nonzero nilpotent element of $\mathbb{Z}[G]$ whose product with the central idempotent $(1 + z)/2$ does not lie in $\mathbb{Z}[G]$, so MJD must fail. Now suppose that all Jordan blocks have dimension one, i.e. t centralizes V. This means there are at least seven central elements of order two in G. If G is not Hamiltonian there will be a cyclic subgroup $\langle x\rangle$ of G and an element y in G with x^y not in $\langle x\rangle$. But then $\alpha = (1 - x)y(1 + x + x^2 + \cdots + x^{k-1})$, where k is the order of x, will be a nonzero nilpotent element of $\mathbb{Z}[G]$. The subgroup $\langle x\rangle$ and its coset $x^y\langle x\rangle$ can together contain at most three central elements of order two; choose a central element z of order two not one of these. Then the product of the central idempotent $(1 + z)/2$ and α will not lie in $\mathbb{Z}[G]$, so again MJD must fail. This completes the proof. $\square$

Lemma 27. *Let G be a finite* 2*-group satisfying the following conditions*:

- *The order of G is at least* 128.
- *G has a maximal subgroup $H = Q_8 \oplus E$, where Q_8 is the quaternion group of order* 8 *and E is an elementary abelian* 2*-group* (*necessarily of rank at least* 3).

- *All maximal subgroups of G are Hamiltonian groups.*
- *G has MJD.*

Then G is a Hamiltonian group.

Proof. Choose t in the complement $G \setminus H$. Arguing as in the previous lemma, we may assume that t centralizes every element of order two in H. Furthermore we may assume that t normalizes (modulo E) at least one of the three cyclic subgroups $\langle x\rangle$, $\langle y\rangle$, $\langle xy\rangle$ of Q_8, say $\langle xy\rangle$. Thus we have that x^t is either x, y, x^3, y^3 or a times one of these, for some a in E. Similarly for y^t, for some b in E, and then $(xy)^t$ will be $xyab$ or $(xy)^3ab$. Consider now the group $K = \langle Q_8, t\rangle$ generated by Q_8 and t. Unless t^2 involves some c in E which is linearly independent of a and b, we will have that $G = K \times E'$ for some nontrivial subgroup E' of E, and then either MJD will fail or G will be Hamiltonian by Corollary 12. The order of t^2 will be either one, two or four. In the first case there is nothing to prove (c does not appear). If t^2 has order four then t will centralize either x or y or xy, so a or b or ab will be 1 and $\langle a, b\rangle$ will have rank at most one, so again we have $G = K \times E'$ as above. Finally, if $t^2 = c$ or $t^2 = x^2c$ for some $c \in E$, and none of a, b, ab are trivial, then t will not normalize the cyclic subgroup $\langle xy\rangle$ of Q_8. Then $\alpha = (1 - xy)t(1 + xy + (xy)^2 + (xy)^3)$ will be nonzero nilpotent and multiplying by the central idempotent $(1 + a)/2$ will give an element not in $\mathbb{Z}[G]$. Hence MJD fails by Corollary 10. □

We are now ready for the main result of this paper.

Theorem 28. *Let G be a group of order* 2^n, $n > 5$. *Then* $\mathbb{Z}[G]$ *has the MJD property if and only if G is a Hamiltonian group.*

Proof. We proceed by induction on the order of G, the assertion being true for groups of order 64 (Theorem 20). Suppose G is a 2-group of order greater than 64 with its integral group ring having the MJD property, and that the result holds for groups of order smaller than that of G. Then, for every proper subgroup H of G, $\mathbb{Z}[H]$ has the MJD property. Therefore, by the induction hypothesis, every maximal subgroup of G is Hamiltonian. In case every maximal subgroup is abelian, then Proposition 21 applies, and one of Theorem 5, Proposition 22, or Lemmas 23, 24, and 25 is contradicted. Thus at least one of the maximal subgroups of G must not be abelian. Lemma 27 then shows that G itself is Hamiltonian, completing the inductive step. □

4. Future directions

In this last section we give a result which may help to focus further work on the property of MJD for integral group rings of finite groups.

Theorem 29. *Let G be a finite group such that* $\mathbb{Z}[G]$ *has MJD. Then one of the following holds*:

(1) *G is either abelian or of the form* $Q_8 \times E \times H$ *where E is an elementary abelian* 2*-group and H is abelian of odd order so that* 2 *has odd multiplicative order* mod $|H|$. (*Such G have AJD and hence MJD for trivial reasons, since* $\mathbb{Q}[G]$ *contains no nilpotents.*)
(2) *G has order* 2^a3^b *for some nonnegative integers a, b.*
(3) $G = Q_8 \times C_p$ *for some prime* $p \geqslant 5$ *so that* 2 *has even multiplicative order* mod p.

(4) *G is the split extension of C_p ($p \geqslant 5$) by a cyclic group $\langle g\rangle$ of order 2^k or 3^k for some $k \geqslant 1$, and g^2 or g^3 acts trivially on C_p.*

Proof. Assume p divides $|G|$, where p is a prime at least 5. We must show G is of type (1), (3) or (4). By Theorem 7, G has a normal abelian subgroup N so that p (and possibly other primes at least 5) divides $|N|$, and the order of G/N is $2^a 3^b$. Since G is solvable, G has a Hall $\{2,3\}$-subgroup S of order $2^a 3^b$. Since the subgroups N and S intersect trivially, we conclude from Corollary 12 that $\mathbb{Q}[S]$ cannot contain nonzero nilpotents and hence S is either abelian or of the form $Q_8 \times E$ where E is an elementary abelian 2-group (no summand of order 3^k can occur since 2 has even order modulo 3).

Suppose first that S acts trivially on N by conjugation, so that $G = N \times S$. If S is abelian, then so is G and we are in Case 1. If 2 has odd order modulo $|N|$ and S is $Q_8 \times E$, then again Case 1 applies. Otherwise, if 2 has even order modulo $|N|$, MJD will fail for G by Corollary 13 unless E is trivial, i.e. $S = Q_8$, and N is cyclic of prime power order. But then Lemma 14 applies so N has prime order and we are in Case 3.

Now suppose that S acts nontrivially on N. Write N as the product of its primary factors $N = N_p \times N_q \times \cdots$. Without loss of generality we may assume S acts nontrivially on N_p. But then by applying Corollary 12 to the subgroups N_q (which is normal) and $\langle N_p, S\rangle$, we conclude that N_q must be trivial so $N = N_p$ must be p-primary.

Next we show that N is elementary abelian. If not, let M be the subgroup of N consisting of those elements of order p with maximal divisibility, i.e. being p^kth powers for largest k. Then M will be normal in G, nontrivial, and strictly smaller than N. We claim that all commutators $[n,s]$ for n in N and s in S must lie in M. For, if $[n,s]$ does not lie in M, then $(1-s)n(1+s+s^2+\cdots+s^{o(s)-1})$ will be a nonzero nilpotent whose product with the central idempotent $\hat{M}/|M|$ (normalized sum of elements of M) does not lie in $\mathbb{Z}[G]$, violating MJD by Corollary 9. Hence all $[n,s]$ lie in M, i.e. $n^s = nm$ for some m in M. From this it follows that M is central (since each element of M is a pth power) and hence that conjugation by any s in S has order p on N, contradicting $|S| = 2^a 3^b$. Thus N must be elementary abelian, i.e. a vector space over $\mathbb{F}_p$.

Suppose some element in S of 2-power order acts nontrivially on N. Choose an element s of minimal order with this property (so s^2 will act trivially), and consider the decomposition of N as an $\langle s\rangle$-module. Since $\langle N, s\rangle$ has MJD, we can again apply Corollary 12 to conclude that N is a simple $\langle s\rangle$-module, and since $\mathbb{F}_p^*$ contains -1 we must have that $N = C_p = \langle c\rangle$. Thus $\langle N, s\rangle$ must be of the form given in Case 4 of the theorem, a split extension of C_p by $C_{2^k} = \langle s\rangle$ with s acting as of order 2. We now consider the rest of S. If x in S has order 2, then either x acts trivially on N or xs acts trivially on N. Using Corollary 12, we conclude that x must be a power of s, so S contains only one element of order two. From what we already know about S, this implies that either the 2-part S_2 of S is cyclic or that $S = S_2 = Q_8$.

Suppose first that S_2 is cyclic. We show that this 2-part is precisely $\langle s\rangle$. If not, G will have a subgroup $H = \langle N, t\rangle$ with $t^2 = s$, t acting as of order 4. But then MJD would fail for $\mathbb{Z}[H]$ by Lemma 18, taking $k = 4$. Hence the 2-part of S is $\langle s\rangle$. We are done with this case unless the 3-part of S is present. Consider an element y of order 3 in S. Then y cannot act trivially on N, again by Corollary 12, so it will be enough to consider the case when y acts as of order 3 so sy will act as of order six on N (and 6 must divide $p-1$). But then $K = \langle N, sy\rangle$ could not have MJD for its integral group ring, again by Lemma 18, taking $k = 6$.

We must still consider the possibility that $S = S_2 = Q_8$, where we take $Q_8 = \langle x, y, z\colon x^2 = y^2 = z^2 = t, t^2 = 1, xy = z, [x,y] = t\rangle$. If t acts nontrivially on N then x acts as of order four, and Lemma 18 again gives a contradiction. Hence t must act trivially and (say) x acts as of order two with y acting trivially. But the resulting G cannot have MJD by Lemma 15. Thus this possibility cannot occur, and G must be as described in Case 4.

The remaining case is when no 2-power element acts nontrivially. Then, again by Corollary 12, S must be a 3-group, necessarily abelian. Repeating the argument from above in the 2-power case, there is a 3-power order element s of minimal order with s acting as of order 3 on N. Now decomposing N as an $\langle s\rangle$-module we again must have only one simple component, either C_p (if 3 divides $p-1$) or $C_p \times C_p$ (if 3 does not divide $p-1$). Arguing as above, in the first case we have that G is the split extension of C_p by a cyclic group $\langle s\rangle$ of 3-power order with s^3 central, as in Case 4 of the theorem. Only the second case remains. It will be enough to show that $\mathbb{Z}[L]$ does not have MJD, where L is the split extension of $N = C_p \times C_p$ by $\langle s\rangle$ of order 3^k, where s acts irreducibly and as of order 3 on N. This determines L up to isomorphism. But our Lemma 16 shows that MJD must fail here, and this completes the proof. □

We conclude with some remarks concerning the various cases of this theorem.

Case 2. This paper has covered all of the 2-groups. The integral group rings of both nonabelian groups of order 27, and of two of the three nonabelian groups of order 12, have MJD. Otherwise little seems to be known.

Case 3. We do not know if these groups ever have MJD for their integral group rings. The first example to investigate would be $Q_8 \times C_5$.

Case 4. The groups in this case of order $2p$ are just the dihedral groups, where it is known that AJD and hence MJD holds for their integral group rings. The groups of order $4p$ in this case are the groups Q_{4p}, where it is also known that MJD holds. For the groups of order $8p$ in this case only partial results are known (see [AHP2]). In particular, MJD for the integral group ring of the group of order 136 is still open. The nonabelian group of order 21 mentioned earlier has MJD for its integral group ring, but for other Case 4 groups of order $3^k p$ we are aware of no results. In general, settling MJD for Case 4 groups seems likely to involve difficult norm equation problems in algebraic number fields.

Acknowledgments

The authors wish to express their thanks for the referee's prompt and thoughtful reading of this paper.

References

[Ar] Satya R. Arora, A study of Jordan decomposition in group rings, PhD thesis, Panjab University, Chandigarh, 1995.

[AHP1] Satya R. Arora, A.W. Hales, I.B.S. Passi, Jordan decomposition and hypercentral units in integral group rings, Comm. Algebra 21 (1993) 25–35.

[AHP2] Satya R. Arora, A.W. Hales, I.B.S. Passi, The multiplicative Jordan decomposition in group rings, J. Algebra 209 (1998) 533–542.

[B] A. Borel, Linear Algebraic Groups, Springer, Berlin, 1991.

[BC] N. Burgoyne, R. Cushman, The decomposition of a linear mapping, Linear Algebra Appl. 8 (1974) 515–519.

[GH] R. Gow, B. Huppert, Degree problems of representation theory over arbitrary fields of characteristic 0: On theorems of Itô and J.G. Thompson, J. Reine Angew. Math. 381 (1987) 136–147.

[HLP] A.W. Hales, I.S. Luthar, I.B.S. Passi, Partial augmentations and Jordan decomposition in group rings, Comm. Algebra 18 (1990) 2327–2341.
[HP] A.W. Hales, I.B.S. Passi, Group rings with Jordan decomposition, Arch. Math. 57 (1991) 21–27.
[HP1] A.W. Hales, I.B.S. Passi, Jordan decomposition, in: I.B.S. Passi (Ed.), Algebra, Some Recent Advances, in: Trends Math., Birkhäuser, Basel, 1999, pp. 75–87.
[HS] M. Hall Jr., J.K. Senior, The Groups of Order 2^n $(n \leqslant 6)$, Macmillan, New York, 1964, 255 p.
[Index16] Index of groups of order 16, available at http://www.math.uga.edu/~lvalero/cohohtml/groups_16_index.htm.
[Index32] Index of groups of order 32, available at http://www.math.uga.edu/~lvalero/cohohtml/groups_32_index.htm.
[Index64] Index of groups of order 64, available at http://www.math.uga.edu/~lvalero/cohohtml/groups_64_index.htm.
[L] T.Y. Lam, A First Course in Noncommutative Rings, second ed., Grad. Texts in Math., vol. 131, Springer, Berlin, 2001.
[LP] Chia-Hsin Liu, D.S. Passman, unpublished.
[Ma] A. Malcev, On solvable Lie algebras, Bull. Acad. Sci. URSS. Sér. Math. (Izv. Akad. Nauk SSSR) 9 (1945) 329–356.
[Par] M.M. Parmenter, Multiplicative Jordan decomposition in integral group rings of groups of order 16, Comm. Algebra 30 (2002) 4789–4797.
[Rédei] L. Rédei, Das schiefe Produkt in der Gruppentheorie, Comment. Math. Helv. 20 (1947) 225–264.
[SWe] M. Shirvani, B.A.F. Wehrfritz, Skew Linear Groups, Cambridge Univ. Press, Cambridge, 1986.
[We] B.A.F. Wehrfritz, Infinite Linear Groups, Springer, Berlin, 1973.